УДК 004.056.5

КЛАССИФИКАЦИЯ И ОЦЕНКА УЯЗВИМОСТЕЙ В БЕСПРОВОДНЫХ СЕТЯХ И МЕТОДЫ ИХ УСТРАНЕНИЯ

БЕГЛЯК ЕКАТЕРИНА ВАЛЕРЬЕВНА,
МАРЦИНКЕВИЧ ВЛАДИСЛАВ АНТОНОВИЧ,
магистранты
РОМАНЮК МАКСИМ ВАЛЕРЬЕВИЧ,
ассистент кафедры «Информатики»
ШАРОНОВА ЕЛЕНА ИВАНОВНА
ассистент кафедры «Вычислительных методов и программирования»
Белорусский Государственный Университет Информатики и Радиоэлектроники

Аннотация: в статье рассматриваются ключевые уязвимости беспроводных корпоративных сетей, возникающие в результате использования устаревших протоколов шифрования, перехвата трафика, атак типа Man-in-the-Middle, недостатков в механизмах аутентификации и проблем безопасности IoT-устройств. Описаны современные методы защиты, включая использование протокола WPA3, технологии 802.1X, систем обнаружения и предотвращения атак (WIPS/WIDS), шифрования трафика и строгих политик контроля доступа. Подчеркивается важность регулярных аудитов безопасности и тестирования на проникновение для минимизации рисков. Статья ориентирована на исследователей и инженеров по кибербезопасности, предлагая аналитический обзор актуальных угроз и эффективных решений для защиты Wi-Fi-сетей.
Ключевые слова: беспроводные сети, корпоративная безопасность, Wi-Fi уязвимости, атаки на сети, защита информации, WPA3, перехват трафика, безопасность IoT, корпоративные угрозы.

CLASSIFICATION AND ASSESSMENT OF VULNERABILITIES IN WIRELESS NETWORKS AND METHODS OF THEIR ELIMINATION

Begliak Ekaterina Vale'evna,
Martsinkevich Uladzislau Antonovich,
Romanuk Maksim Vale'evich,
Sharonova Elena Ivanovna

Abstract: the article examines key vulnerabilities in corporate wireless networks arising from the use of outdated encryption protocols, traffic interception, Man-in-the-Middle attacks, authentication weaknesses, and security risks associated with IoT devices. Modern security methods are described, including the use of the WPA3 protocol, 802.1X technology, intrusion detection and prevention systems (WIPS/WIDS), traffic encryption and strict access control policies. The importance of regular security audits and penetration testing to minimize risks is emphasized. The article is intended for researchers and cybersecurity engineers, offering an analytical overview of current threats and effective solutions for securing Wi-Fi networks.
Keywords: wireless networks, corporate security, Wi-Fi vulnerabilities, network attacks, information protection, WPA3, traffic interception, IoT security, corporate threats, protection methods.

Беспроводные корпоративные сети представляют собой удобный инструмент для работы сотрудников и подключения устройств, но их открытая природа делает их уязвимыми перед различными атаками. С ростом использования беспроводных технологий значительно увеличиваются и угрозы безопасности, связанные с ними. Уязвимости беспроводных сетей могут привести к различным рискам, включая несанкционированный доступ, перехват данных и вмешательство в работу сети. Для эффективной защиты информации важно изучать различные типы угроз и методы их классификации, которые можно разделить на несколько категорий, каждая из которых требует особого подхода.

1. Уязвимости в протоколах беспроводных сетей

Одной из самых распространенных проблем является использование устаревших протоколов шифрования. Ранее популярный WEP оказался настолько уязвимым, что его можно взломать за считанные минуты, просто проанализировав сетевой трафик. Исследователи из Вашингтонского университета показали, что WEP можно взломать всего за 3-5 минут, проанализировав около 100-150 тысяч пакетов данных [1]. WPA и WPA2, несмотря на улучшенные механизмы защиты, также имеют уязвимости. Например, атака KRACK позволяет злоумышленнику перехватывать данные, передаваемые между клиентом и точкой доступа, даже если используется современный WPA2. Новый стандарт WPA3 призван устранить многие слабые места, но исследования показали, что и он подвержен атакам, таким как Dragonblood, позволяющим снижать уровень защиты соединения [2].

2. Физические уязвимости

Поскольку передача данных в беспроводных сетях происходит через открытый канал, злоумышленники могут легко перехватывать и анализировать трафик. Глушение (Jamming) является еще одной распространенной угрозой, когда вредоносные устройства создают помехи, что приводит к деградации или прекращению связи. Атака повторного воспроизведения (Replay attacks) также представляют собой значительную угрозу: злоумышленники могут записывать сетевой трафик и повторно отправлять его для достижения каких-либо целей, таких как повторный вход в систему.

Серьезной угрозой являются атаки, основанные на перехвате трафика, такие как создание «злой двойник» (Evil Twin). Злоумышленники настраивают поддельную Wi-Fi-точку с таким же именем (SSID), как у корпоративной сети, и пользователи, не подозревая о подмене, подключаются к ней, передавая все свои данные атакующему. Подобные атаки могут проводиться и с использованием Rogue AP – незарегистрированных точек доступа, установленных внутри организации. Эти точки могут использоваться для атак типа Man-in-the-Middle, когда злоумышленник получает возможность прослушивать, изменять и подменять сетевой трафик [3, с. 189]. Последнюю уязвимость в некоторой степени можно отнести и к следующей категории.

3. Атаки на аутентификацию

Атаки на пароли представляют собой серьезную угрозу, так как простые или слабые пароли могут быть легко взломаны с использованием метода перебора. Даже если используется WPA2, а пароль слабый, злоумышленник может его подобрать методом перебора (brute-force) или с использованием атак словарного типа. В корпоративных сетях, использующих WPA2-Enterprise, хотя этот режим предусматривает централизованную аутентификацию через RADIUS-сервер, ошибки конфигурации или слабая реализация протоколов аутентификации (например, EAP) могут позволить злоумышленнику получить учетные данные сотрудников [4, с, 165].

4. Уязвимости в устройствах и программном обеспечении

Устаревшие устройства и небезопасные прошивки могут содержать уязвимости, которые злоумышленники могут использовать для атак. Недостаток обновлений безопасности делает такие устройства легкой мишенью. Уязвимости в драйверах и программных компонентах также могут быть использованы для компрометации устройства, подключающегося к беспроводной сети.

Дополнительный уровень угроз создают IoT-устройства, а также политика BYOD (Bring Your Own Device), когда сотрудники подключают к корпоративной сети личные устройства. Многие IoT-устройства, такие как камеры наблюдения, принтеры или умные датчики, не имеют достаточного уровня защиты – их пароли по умолчанию легко подбираются, а шифрование часто отсутствует. Кроме того, личные ноутбуки и смартфоны сотрудников могут быть заражены вредоносным ПО, которое затем

распространяется в корпоративной сети.

5. Уязвимости в управлении сетью

Некорректно сконфигурированные настройки безопасности, такие как шифрование и аутентификация, могут сделать сеть уязвимой. Также открытые или устаревшие точки доступа могут быть использованы злоумышленниками для доступа к сети [5, с. 150].

Отдельной проблемой становится недостаточный мониторинг беспроводных сетей. Если организация не использует специализированные системы обнаружения вторжений (WIDS/WIPS), то атаки могут оставаться незамеченными до момента утечки данных или проникновения злоумышленников в сеть. Регулярные тесты на проникновение и анализ конфигурации точек доступа также часто игнорируются, что дает злоумышленникам возможность воспользоваться давно известными уязвимостями.

Таким образом, беспроводные корпоративные сети подвержены множеству угроз, начиная от слабых алгоритмов шифрования и атак на аутентификацию, заканчивая использованием уязвимых IoT-устройств и недостаточным контролем доступа. Однако существуют эффективные методы устранения этих проблем, которые позволяют значительно повысить безопасность беспроводных сетей [6, с. 465].

Обеспечение безопасности беспроводной сети – это сложная задача, требующая использования современных протоколов шифрования, эффективного контроля доступа и постоянного мониторинга активности в сети. Одним из ключевых шагов является переход на WPA3 – новый стандарт безопасности Wi-Fi, который решает проблемы, связанные с атаками на аутентификацию и перехватом данных. В отличие от предыдущих стандартов, WPA3 использует более надежный алгоритм SAE (Simultaneous Authentication of Equals), который делает атаки словарного перебора практически невозможными.

Однако одного лишь обновления стандарта недостаточно. Важным шагом является внедрение 802.1X с EAP-TLS – технологии, обеспечивающей аутентификацию пользователей на основе цифровых сертификатов. Это исключает возможность использования слабых паролей и снижает риск атак Evil Twin, поскольку злоумышленнику становится гораздо сложнее подделать сервер аутентификации. Кроме того, организациям следует полностью отказаться от устаревших протоколов WEP, WPA и TKIP, так как они уже давно признаны ненадежными.

Контроль доступа – еще один важный элемент защиты корпоративных сетей. Для минимизации рисков рекомендуется использовать VLAN (виртуальные локальные сети), позволяющие изолировать различные типы устройств. Например, IoT-устройства, работающие в компании, должны быть подключены к отдельной сети, не имеющей доступа к основным корпоративным ресурсам. Подход Zero Trust Network (ZTN) также набирает популярность: он предполагает, что даже внутри организации пользователи и устройства должны проходить строгую аутентификацию перед получением доступа к данным [6].

Атаки типа Evil Twin и Rogue AP могут быть предотвращены с помощью систем WIPS (Wireless Intrusion Prevention System), которые анализируют радиоэфир и автоматически блокируют подозрительные точки доступа. Также рекомендуется использовать корпоративные VPN-сервисы для защиты передаваемого трафика, особенно при работе из общественных мест или удаленных офисов.

Помимо защиты сети, важно уделять внимание безопасности устройств, подключенных к ней. IoT-устройства должны использовать сложные пароли, а их прошивки необходимо регулярно обновлять. Также следует отключать ненужные сервисы, такие как Telnet или UPnP, которые могут быть использованы злоумышленниками для удаленного управления устройствами. В организациях, где сотрудники используют личные устройства (BYOD), необходимо внедрение систем MDM (Mobile Device Management), которые позволяют контролировать уровень безопасности подключаемых устройств и применять централизованные политики защиты [6, с. 452].

Регулярные аудиты безопасности – еще одна важная мера, позволяющая выявить уязвимости до того, как ими воспользуются злоумышленники. Сканирование сети с использованием инструментов вроде Nmap и Nessus поможет обнаружить незащищенные точки доступа, а тестирование на проникновение (Pentesting) позволит смоделировать реальные атаки и выявить слабые места системы защиты. Помимо технических мер, не стоит забывать и о человеческом факторе: сотрудники должны проходить регулярное обучение по кибербезопасности, чтобы не становиться жертвами атак, связанных с социальной инженерией.

Безопасность беспроводных корпоративных сетей требует комплексного подхода. В статье были рассмотрены основные уязвимости, включая слабые протоколы шифрования, атаки типа Man-in-the-Middle, проблемы аутентификации и угрозы со стороны IoT-устройств. Для устранения этих рисков рекомендуется переход на современные стандарты безопасности, использование WIPS/WIDS, VPN, сегментацию сети и регулярные аудиты безопасности.

Применение данных методов позволяет значительно снизить вероятность атак и обеспечить защиту корпоративных данных. В будущем следует учитывать развитие новых угроз и адаптировать стратегии защиты в соответствии с актуальными вызовами информационной безопасности.

Список источников

1. Wireless LAN Security II: WEP Attacks, WPA and WPA2 [Электронный ресурс]. – Режим доступа: URL: https://www.cse.wustl.edu/~jain/cse571-09/ftp/l_20wpa.pdf – (23.02.2025)
2. Wireless Security Protocols WPA3: A Systematic Literature Review [Электронный ресурс]. – Режим доступа: URL: https://ieeexplore.ieee.org/document/10274082 (24.02.2025)
3. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – Москва : ДМК Пресс, 2023. – 440 с.
4. Analysis of attacks in IEEE 802.11 networks at different levels of OSI model / R. Yu. Korolkov [и др.] / Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. – 2021. – №2. – с. 163-168
5. Гейер, Дж. Беспроводные сети. Первый шаг: Пер. с англ. / Дж. Гейер. – Москва : Издательский дом "Вильяме", 2005. – 192 с.
6. Minella, J. Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise / J. Minella. – Hoboken : John Wiley & Sons, 2022. – 624 с.